

What is claimed is:

1 1. A key agreement system comprising a shared-key
2 generation apparatus and a shared-key recovery apparatus,
3 each apparatus establishing therein a same shared key in
4 secrecy, wherein
5 the shared-key generation apparatus includes:
6 a seed-value generating unit operable to generate
7 a seed value;
8 a first shared-key generating unit operable to
9 generate a blind value and a shared key, from the seed value;
10 an encryption unit operable to encrypt the seed
11 value based on the blind value, to generate encryption
12 information; and
13 a transmitting unit operable to transmit the
14 encryption information, and
15 the shared-key recovery apparatus includes:
16 a receiving unit operable to receive the
17 encryption information;
18 a decryption unit operable to decrypt the
19 encryption information, to generate a decryption seed
20 value;
21 a second shared-key generating unit operable to
22 generate a decryption blind value and a decryption shared

23 key, using the decryption seed value and according to a
24 same method as used in the first shared-key generating unit;
25 a re-encryption unit operable to encrypt the
26 decryption seed value based on the decryption blind value,
27 to generate re-encryption information;
28 a judging unit operable to judge, based on the
29 encryption information and the re-encryption information,
30 whether the decryption shared key should be outputted; and
31 an outputting unit operable, when the judging unit
32 has judged affirmatively, to output the decryption shared
33 key.

1 2. The key agreement system of Claim 1, wherein
2 the shared-key generation apparatus further
3 includes:
4 an obtaining unit operable to obtain a content;
5 and
6 an encryption unit operable to encrypt the
7 obtained content using the shared key, to generate
8 an encrypted content,
9 the transmitting unit further transmits the encrypted
10 content,
11 the receiving unit further receives the encrypted
12 content, and

13 the shared-key recovery apparatus further includes:
14 a decryption unit operable to decrypt the
15 received encrypted content using the decryption
16 shared key, to generate a decrypted content; and
17 an outputting unit operable to output the
18 decrypted content.

1 3. A shared-key generation apparatus that notifies a
2 destination apparatus about a shared key in secrecy, the
3 shared-key generation apparatus comprising:
4 a seed-value generating unit operable to generate a
5 seed value;
6 a shared-key generating unit operable to generate a
7 blind value and a shared key, from the seed value;
8 an encryption unit operable to encrypt the seed value
9 based on the blind value, to generate encryption
10 information; and
11 a transmitting unit operable to transmit the
12 encryption information.

1 4. The shared-key generation apparatus of Claim 3,
2 wherein
3 the shared-key generating unit performs a one-way
4 function on the seed value, to generate a functional value,

5 and generates the blind value and the shared key from the
6 functional value,
7 the encryption unit includes:
8 a public-key obtaining subunit operable to obtain
9 a public key; and
10 a public-key encryption subunit operable to
11 perform a public-key encryption algorithm on the seed value,
12 using the public key and the blind value, to generate an
13 encryption seed value as the encryption information.

1 5. The shared-key generation apparatus of Claim 4,
2 wherein
3 the public-key encryption algorithm conforms to an
4 NTRU cryptosystem,
5 the public-key obtaining subunit obtains a public-key
6 polynomial generated according to a key-generation
7 algorithm of the NTRU cryptosystem, as the public key,
8 the public-key encryption subunit generates a
9 seed-value polynomial from the seed value, generates a
10 blind-value polynomial from the blind value, and encrypts
11 the seed-value polynomial according to an encryption
12 algorithm of the NTRU cryptosystem, using the public-key
13 polynomial as a key, and using the blind-value polynomial
14 to randomize the seed-value polynomial, to generate an

15 encryption seed-value polynomial as the encryption seed
16 value, and
17 the transmitting unit transmits the encryption
18 seed-value polynomial as the encryption seed value.

1 6. The shared-key generation apparatus of Claim 3,
2 wherein

3 the encryption unit includes:

4 a public-key obtaining subunit operable to obtain
5 a public key;

6 a public-key encryption subunit operable to
7 generate a blind value, perform the public-key encryption
8 algorithm on the seed value using the public key and the
9 blind value, to generate a public-key cipher text; and

10 a function subunit operable to perform a second
11 one-way function on at least one of the seed value, the
12 blind value, and the shared key, to generate a second
13 functional value, and

14 the encryption unit generates the encryption
15 information that includes the public-key cipher text and
16 the second functional value.

1 7. The shared-key generation apparatus of Claim 6,
2 wherein

3 the shared-key generating unit performs a one-way
4 function on the seed value, to generate a functional value,
5 and generates the blind value and the shared key from the
6 functional value.

1 8. The shared-key generation apparatus of Claim 6,
2 wherein

3 the shared-key generating unit performs a first
4 one-way function on the seed value, to generate a first
5 functional value, and generates the shared key from the
6 first functional value, instead of generating the blind
7 value and the shared key.

1 9. The shared-key generation apparatus of Claim 6,
2 wherein

3 the public-key encryption algorithm conforms to an
4 NTRU cryptosystem,

5 the public-key obtaining subunit obtains a public-key
6 polynomial generated according to a key-generation
7 algorithm of the NTRU cryptosystem, as the public key,
8 the public-key encryption subunit generates a
9 seed-value polynomial from the seed value, generates a
10 blind-value polynomial from the blind value, encrypts the
11 seed-value polynomial according to an encryption algorithm

12 of the NTRU cryptosystem, using the public-key polynomial
13 as a key, and using the blind-value polynomial to randomize
14 the seed-value polynomial, to generate an encryption
15 seed-value polynomial as the public-key cipher text, and
16 the encryption unit generates the encryption
17 information that includes the encryption seed-value
18 polynomial as the public-key cipher text and the second
19 functional value.

1 10. The shared-key generation apparatus of Claim 3,
2 wherein

3 the shared-key generating unit performs a one-way
4 function on the seed value, to generate a functional value,
5 and generates a verification value, the blind value, and
6 the shared key, from the functional value,

7 the encryption unit includes:

8 a public-key obtaining subunit operable to obtain
9 a public key;

10 a first encryption subunit operable to perform a
11 public-key encryption algorithm on the verification value,
12 using the public key and the blind value, to generate a
13 first cipher text; and

14 a second encryption subunit operable to perform,
15 on the seed value, a computation algorithm different from

16 the public-key encryption algorithm, to generate a second
17 cipher text, and
18 the encryption unit generates the encryption
19 information that includes the first cipher text and the
20 second cipher text.

1 11. The shared-key generation apparatus of Claim 10,
2 wherein
3 the public-key encryption algorithm conforms to an
4 NTRU cryptosystem,
5 the public-key obtaining subunit obtains a public-key
6 polynomial generated according to a key-generation
7 algorithm of the NTRU cryptosystem, as the public key,
8 the first encryption subunit generates a
9 verification-value polynomial from the verification value,
10 generates a blind-value polynomial from the blind value,
11 and encrypts the verification-value polynomial according
12 to an encryption algorithm of the NTRU cryptosystem, using
13 the public-key polynomial as a key, and using the blind-value
14 polynomial to randomize the verification-value polynomial,
15 to generate an encryption verification-value polynomial
16 as the first cipher text, and
17 the encryption unit generates the encryption
18 information that includes the encryption

19 verification-value polynomial as the first cipher text and
20 the second cipher text.

1 12. The shared-key generation apparatus of Claim 11,
2 wherein
3 the different computation algorithm is a symmetric
4 key encryption algorithm, and
5 the second encryption subunit performs the symmetric
6 key encryption algorithm on the seed value using the
7 verification value as a key, to generate the second cipher
8 text.

1 13. The shared-key generation apparatus of Claim 11,
2 wherein
3 the different computation algorithm is bitwise
4 exclusive-or, and
5 the second encryption subunit performs the bitwise
6 exclusive-or on the verification value and the seed value,
7 to generate the second cipher text.

1 14. The shared-key generation apparatus of Claim 11,
2 wherein
3 the different computation algorithm is addition, and
4 the second encryption subunit performs the addition

5 on the verification value and the seed value, to generate
6 the second cipher text.

1 15. The shared-key generation apparatus of Claim 11,
2 wherein

3 the different computation algorithm is
4 multiplication, and

5 the second encryption subunit performs the
6 multiplication on the verification value and the seed value,
7 to generate the second cipher text.

1 16. The shared-key generation apparatus of Claim 3,
2 wherein

3 the seed-value generating unit generates a random
4 number, as the seed value.

1 17. The shared-key generation apparatus of Claim 3,
2 wherein

3 the shared-key generating unit performs a one-way
4 function on the seed value, to generate a functional value,
5 and generates the blind value and the shared key from the
6 functional value.

1 18. The shared-key generation apparatus of Claim 17,

2 wherein
3 the one-way function is a hash function, and
4 the shared-key generating unit performs the hash
5 function on the seed value.

1 19. The shared-key generation apparatus of Claim 17,
2 wherein
3 the shared-key generating unit generates the blind
4 value by setting a part of the functional value as the blind
5 value, and generates the shared key by setting another part
6 of the functional value as the shared key.

1 20. The shared-key generation apparatus of Claim 3,
2 further comprising:
3 an obtaining unit operable to obtain a content; and
4 an encryption unit operable to encrypt the obtained
5 content using the shared key, to generate an encrypted
6 content, wherein
7 the transmitting unit further transmits the encrypted
8 content.

1 21. A shared-key recovery apparatus that receives a shared
2 key from a shared-key generation apparatus in secrecy, the
3 shared-key generation apparatus generating a seed value,

4 generating a blind value and a shared key from the seed
5 value, encrypting the seed value based on the blind value
6 to generate encryption information, and transmitting the
7 encryption information, the shared-key recovery apparatus
8 comprising:
9 a receiving unit operable to receive the encryption
10 information;
11 a decryption unit operable to decrypt the encryption
12 information, to generate a decryption seed value;
13 a shared-key generating unit operable to generate a
14 decryption blind value and a decryption shared key, using
15 the decryption seed value and according to a same shared-key
16 generating method used in the shared-key generation
17 apparatus;
18 a re-encryption unit operable to encrypt the
19 decryption seed value based on the decryption blind value,
20 to generate re-encryption information;
21 a judging unit operable to judge, based on the
22 encryption information and the re-encryption information,
23 whether the decryption shared key should be outputted; and
24 an outputting unit operable, when the judging unit
25 has judged affirmatively, to output the decryption shared
26 key.

1 22. The shared-key recovery apparatus of Claim 21, wherein
2 the shared-key generation apparatus performs a
3 one-way function on the seed value to generate a functional
4 value, generates the blind value and the shared key from
5 the functional value, obtains a public key, performs a
6 public-key encryption algorithm on the seed value using
7 the public key and the blind value, to generate an encryption
8 seed value as the encryption information, and transmits
9 the encryption seed value,
10 the receiving unit receives the encryption seed value
11 as the encryption information,
12 the decryption unit includes:
13 a secret-key obtaining subunit operable to obtain
14 a secret key that corresponds to the public key; and
15 a public-key decryption subunit operable to
16 perform, on the received encryption seed value, a public-key
17 decryption algorithm that corresponds to the public-key
18 encryption algorithm, using the obtained secret key, to
19 generate the decryption seed value,
20 the shared-key generating unit performs the one-way
21 function on the decryption seed value to generate a
22 decryption functional value, and generates the decryption
23 blind value and the decryption shared key from the decryption
24 functional value,

25 the re-encryption unit includes:
26 a public-key obtaining subunit operable to obtain
27 the public key; and
28 a re-encryption subunit operable to perform the
29 public-key encryption algorithm on the decryption seed
30 value using the public key and the decryption blind value,
31 to generate a re-encryption seed value as the re-encryption
32 information, and
33 the judging unit judges whether the encryption seed
34 value is identical to the re-encryption seed value, and
35 when judging affirmatively, determines that the decryption
36 shared key should be outputted.

1 23. The shared-key recovery apparatus of Claim 22, wherein
2 the public-key encryption algorithm and the
3 public-key decryption algorithm conform to an NTRU
4 cryptosystem,
5 the shared-key generation apparatus obtains a
6 public-key polynomial generated according to a
7 key-generation algorithm of the NTRU cryptosystem, as the
8 public key, generates a seed-value polynomial from the seed
9 value, generates a blind-value polynomial from the blind
10 value, encrypts the seed-value polynomial according to an
11 encryption algorithm of the NTRU cryptosystem, using the

12 public-key polynomial as a key, and using the blind-value
13 polynomial to randomize the seed-value polynomial, to
14 generate an encryption seed-value polynomial as the
15 encryption seed value, and transmits the encryption
16 seed-value polynomial as the encryption seed value,
17 the receiving unit receives the encryption seed-value
18 polynomial as the encryption seed value,
19 the secret-key obtaining subunit obtains a secret-key
20 polynomial generated according to the key-generation
21 algorithm of the NTRU cryptosystem, as the secret key,
22 the public-key decryption subunit decrypts the
23 received encryption seed-value polynomial according to a
24 decryption algorithm of the NTRU cryptosystem and using
25 the obtained secret-key polynomial as a key, to generate
26 a decryption seed-value polynomial, and generates the
27 decryption seed value from the decryption seed-value
28 polynomial,
29 the public-key obtaining subunit obtains the
30 public-key polynomial as the public key,
31 the re-encryption subunit generates a seed-value
32 polynomial from the decryption seed value, generates a
33 blind-value polynomial from the decryption blind value,
34 and encrypts the seed-value polynomial according to the
35 encryption algorithm of the NTRU cryptosystem, using the

36 public-key polynomial as a key, and using the blind-value
37 polynomial to randomize the seed-value polynomial, to
38 generate a re-encryption seed-value polynomial, and
39 the judging unit judges whether the encryption
40 seed-value polynomial is identical to the re-encryption
41 seed-value polynomial.

1 24. The shared-key recovery apparatus of Claim 21, wherein
2 the shared-key generation apparatus obtains a public
3 key, generates a blind value, performs a public-key
4 encryption algorithm on the seed value using the public
5 key and the blind value to generate a public-key cipher
6 text, performs a second one-way function on at least one
7 of the seed value, the blind value, and the shared key to
8 generate a second functional value, generates the
9 encryption information that includes the public-key cipher
10 text and the second functional value, and transmits the
11 encryption information,

12 the receiving unit receives the encryption
13 information that includes the public-key cipher text and
14 the second functional value,

15 the decryption unit includes:

16 a secret-key obtaining subunit operable to obtain
17 a secret key that corresponds to the public key;

18 a public-key decryption subunit operable to
19 perform, on the public-key cipher text included in the
20 received encryption information, a public-key decryption
21 algorithm that corresponds to the public-key encryption
22 algorithm, to generate a decryption seed value; and

23 a function subunit operable to perform the second
24 one-way function on at least one of the decryption seed
25 value, the decryption blind value, and the decryption shared
26 key, to generate a decryption second functional value, and

27 the judging unit judges whether the second functional
28 value included in the received encryption information is
29 identical to the decryption second functional value instead
30 of performing judging based on the encryption information
31 and the re-encryption information, and when judging
32 affirmatively, determines that the decryption shared key
33 should be outputted.

1 25. The shared-key recovery apparatus of Claim 24, wherein
2 the shared-key generation apparatus performs a
3 one-way function on the seed value to generate a functional
4 value, and generates the blind value and the shared key
5 from the functional value, and
6 the shared-key generating unit performs the first
7 one-way function on the decryption seed value to generate

8 a decryption functional value, and generates the decryption
9 blind value and the decryption shared key from the decryption
10 functional value.

1 26. The shared-key recovery apparatus of Claim 24, wherein
2 the shared-key generation apparatus performs a first
3 one-way function on the seed value to generate a first
4 functional value, and generates the shared key from the
5 first functional value, instead of generating the blind
6 value and the shared key, and

7 the shared-key generating unit performs the first
8 one-way function on the decryption seed value to generate
9 a decryption functional value, and generates the decryption
10 shared key from the decryption functional value, instead
11 of generating the decryption blind value and the decryption
12 shared key.

1 27. The shared-key recovery apparatus of Claim 24, wherein
2 the public-key encryption algorithm and the
3 public-key decryption algorithm conform to an NTRU
4 cryptosystem,

5 the shared-key generation apparatus obtains a
6 public-key polynomial generated according to a
7 key-generation algorithm of the NTRU cryptosystem, as the

8 public key, generates a seed-value polynomial from the seed
9 value, generates a blind-value polynomial from the blind
10 value, encrypts the seed-value polynomial according to an
11 encryption algorithm of the NTRU cryptosystem using the
12 public-key polynomial as a key and using the blind-value
13 polynomial to randomize the seed-value polynomial, to
14 generate an encryption seed-value polynomial as the
15 public-key cipher text, and generates the encryption
16 information that includes the encryption seed-value
17 polynomial as the public-key cipher text and the second
18 functional value,

19 the secret-key obtaining subunit obtains a secret-key
20 polynomial generated according to the key-generation
21 algorithm of the NTRU cryptosystem, as the secret key, and

22 the public-key decryption subunit generates a
23 public-key cipher-text polynomial from the public-key
24 ciphertext, decrypts the public-key cipher-text polynomial
25 according to a decryption algorithm of the NTRU cryptosystem
26 using the secret-key polynomial as a key to generate a
27 decryption seed-value polynomial, and generates the
28 decryption seed value from the decryption seed-value
29 polynomial.

1 28. The shared-key recovery apparatus of Claim 21, wherein

2 the shared-key generation apparatus performs a
3 one-way function on the seed value to generate a functional
4 value, generates a verification value, the blind value,
5 and the shared key from the functional value, obtains a
6 public key, performs a public-key encryption algorithm on
7 the verification value using the public key and the blind
8 value to generate a first cipher text, performs, based on
9 the verification value, a computation algorithm different
10 from the public-key encryption algorithm on the seed value,
11 to generate a second cipher text, generates the encryption
12 information that includes the first cipher text and the
13 second cipher text, and transmits the encryption
14 information,

15 the receiving unit receives the encryption
16 information that includes the first cipher text and the
17 second cipher text,

18 the decryption unit includes:

19 a secret-key obtaining subunit operable to obtain
20 a secret key that corresponds to the public key;

21 a public-key decryption subunit operable to
22 perform, on the first cipher text included in the received
23 encryption information, a public-key decryption algorithm
24 that corresponds to the public-key encryption algorithm,
25 to generate a decryption verification value; and

26 a computation decryption subunit operable to
27 perform, on the second cipher text included in the received
28 encryption information, a computation algorithm for
29 performing an inverse computation of the different
30 computation algorithm, to generate a decryption seed value,
31 the shared-key generating unit performs the one-way
32 function on the decryption seed value to generate a
33 decryption functional value, and generates a decryption
34 verification value, the decryption blind value, and the
35 decryption shared key, from the decryption functional
36 value,
37 the re-encryption unit includes:
38 a public-key obtaining subunit operable to obtain
39 the public key; and
40 a re-encryption subunit operable to perform, on
41 the decryption verification value, the public-key
42 encryption algorithm using the public key and the decryption
43 blind value, to generate the re-encryption information,
44 and
45 the judging unit judges whether the first cipher
46 text included in the encryption information is identical
47 to the re-encryption information, and when judging
48 affirmatively, determines that the decryption shared key
49 should be outputted.

1 29. The shared-key recovery apparatus of Claim 28, wherein
2 the public-key encryption algorithm and the
3 public-key decryption algorithm conform to an NTRU
4 cryptosystem,
5 the shared-key generation apparatus obtains a
6 public-key polynomial generated according to a
7 key-generation algorithm of the NTRU cryptosystem, as the
8 public key, generates a verification-value polynomial from
9 the verification value, generates a blind-value polynomial
10 from the blind value, encrypts the verification-value
11 polynomial according to an encryption algorithm of the NTRU
12 cryptosystem, using the public-key polynomial as a key,
13 and using the blind-value polynomial to randomize the
14 verification-value polynomial, to generate an encryption
15 verification-value polynomial as the first cipher text,
16 generates the encryption information that includes the
17 encryption verification-value polynomial as the first
18 cipher text and the second cipher text, and transmits the
19 encryption information,
20 the receiving unit receives the encryption
21 information that includes the encryption
22 verification-value polynomial and the second cipher text,
23 the secret-key obtaining subunit obtains a secret-key
24 polynomial generated according to the key-generation

25 algorithm of the NTRU cryptosystem, as the secret key,
26 the public-key decryption subunit generates a first
27 cipher-text polynomial from the first cipher text, decrypts
28 the first cipher-text polynomial according to a decryption
29 algorithm of the NTRU cryptosystem using the secret-key
30 polynomial as a key, to generate a decryption verification
31 polynomial, and generates the decryption verification value
32 from the decryption verification-value polynomial,
33 the public-key obtaining subunit obtains the
34 public-key polynomial,
35 the re-encryption subunit generates a decryption
36 verification-value polynomial from the decryption
37 verification value, generates a blind-value polynomial from
38 the decryption blind value, and encrypts the decryption
39 verification-value polynomial according to the encryption
40 algorithm of the NTRU cryptosystem, using the public-key
41 polynomial as a key, and using the blind-value polynomial
42 to randomize the decryption verification-value polynomial,
43 to generate a re-encryption verification-value polynomial
44 as the re-encryption information, and
45 the judging unit judges whether the encryption
46 verification-value polynomial as the first cipher text is
47 identical to the re-encryption verification-value
48 polynomial as the re-encryption information.

1 30. The shared-key recovery apparatus of Claim 29, wherein
2 the different computation algorithm is a symmetric
3 key encryption algorithm, and the computation algorithm
4 for performing the inverse computation is a corresponding
5 symmetric key decryption algorithm, and
6 the computation decryption subunit performs the
7 symmetric key decryption algorithm on the second cipher
8 text, using the decryption verification value as a key,
9 to generate the decryption seed value.

1 31. The shared-key recovery apparatus of Claim 29, wherein
2 the different computation algorithm and the
3 computation algorithm for performing the inverse
4 computation are bitwise exclusive-or, and
5 the computation decryption subunit performs the
6 bitwise exclusive-or on the decryption verification value
7 and the second cipher text, to generate the decryption seed
8 value.

1 32. The shared-key recovery apparatus of Claim 29, wherein
2 the different computation algorithm is addition and
3 the computation algorithm for performing the inverse
4 computation is subtraction, and
5 the computation decryption subunit performs the

6 subtraction on the decryption verification value and the
7 second cipher text, to generate the decryption seed value.

1 33. The shared-key recovery apparatus of Claim 29, wherein
2 the different calculation algorithm is
3 multiplication and the computation algorithm for performing
4 the inverse computation is division, and
5 the computation decryption subunit performs the
6 division on the decryption verification value and the second
7 cipher text, to generate the decryption seed value.

1 34. The shared-key recovery apparatus of Claim 21, wherein
2 the shared-key generating unit performs a one-way
3 function on the decryption seed value to generate a
4 functional value, and generates the decryption blind value
5 and the decryption shared key from the functional value.

1 35. The shared-key recovery apparatus of Claim 34, wherein
2 the one-way function is a hash function, and the
3 shared-key generating unit performs the hash function on
4 the decryption seed value.

1 36. The shared-key recovery apparatus of Claim 34, wherein
2 the shared-key generating unit generates the

3 decryption blind value by setting a part of the functional
4 value as the decryption blind value, and generates the
5 decryption shared key by setting another part of the
6 functional value as the decryption shared key.

1 37. The shared-key recovery apparatus of Claim 21, wherein
2 the shared-key generation apparatus further obtains
3 a content, encrypts the obtained content using the shared
4 key to generate an encrypted content, and transmits the
5 encrypted content, and
6 the shared-key recovery apparatus further includes:
7 a content receiving unit operable to receive the
8 encrypted content;
9 a decryption unit operable to decrypt the received
10 encrypted content using the outputted decryption shared
11 key, to generate a decrypted content; and
12 a playback unit operable to playback the decrypted
13 content.

1 38. A shared-key generating method used in a shared-key
2 generation apparatus that notifies a destination apparatus
3 about a shared key in secrecy, the shared-key generating
4 method comprising:
5 a seed-value generating step of generating a seed

6 value;
7 a shared-key generating step of generating a blind
8 value and a shared key, from the seed value;
9 an encryption step of encrypting the seed value based
10 on the blind value, to generate encryption information;
11 and
12 a transmitting step of transmitting the encryption
13 information.

1 39. A shared-key generating program used in a shared-key
2 generation apparatus that notifies a destination apparatus
3 about a shared key in secrecy, the shared-key generating
4 program comprising:

5 a seed-value generating step of generating a seed
6 value;
7 a shared-key generating step of generating a blind
8 value and a shared key, from the seed value;
9 an encryption step of encrypting the seed value based
10 on the blind value, to generate encryption information;
11 and
12 a transmitting step of transmitting the encryption
13 information.

1 40. The shared-key generating program of Claim 39, wherein

the shared-key generating program is recorded in a computer-readable recording medium.

41. A shared-key recovery method used in a shared-key recovery apparatus that receives a shared key from a shared-key generation apparatus in secrecy, the shared-key generation apparatus generating a seed value, generating a blind value and a shared key from the seed value, encrypting the seed value based on the blind value to generate encryption information, and transmitting the encryption information, the shared-key recovery method comprising:

a receiving step of receiving the encryption information;

a decryption step of decrypting the encryption information, to generate a decryption seed value;

a shared-key generating step of generating a decryption blind value and a decryption shared key, using the decryption seed value and according to a same shared-key generating method used in the shared-key generation apparatus;

a re-encryption step of encrypting the decryption seed value based on the decryption blind value, to generate re-encryption information;

a judging step of judging, based on the encryption

22 information and the re-encryption information, whether the
23 decryption shared key should be outputted; and
24 an outputting step, when the judging unit has judged
25 affirmatively, of outputting the decryption shared key.

1 42. A shared-key recovery program used in a shared-key
2 recovery apparatus that receives a shared key from a
3 shared-key generation apparatus in secrecy, the shared-key
4 generation apparatus generating a seed value, generating
5 a blind value and a shared key from the seed value, encrypting
6 the seed value based on the blind value to generate encryption
7 information, and transmitting the encryption information,
8 the shared-key recovery program comprising:

9 a receiving step of receiving the encryption
10 information;

11 a decryption step of decrypting the encryption
12 information, to generate a decryption seed value;

13 a shared-key generating step of generating a
14 decryption blind value and a decryption shared key, using
15 the decryption seed value and according to a same shared-key
16 generating method used in the shared-key generation
17 apparatus;

18 a re-encryption step of encrypting the decryption seed
19 value based on the decryption blind value, to generate

20 re-encryption information;
21 a judging step of judging, based on the encryption
22 information and the re-encryption information, whether the
23 decryption shared key should be outputted; and
24 an outputting step, when the judging unit has judged
25 affirmatively, of outputting the decryption shared key.

1 43. The shared-key recovery program of Claim 42, wherein
2 The shared-key recovery program is recorded in a
3 computer-readable recording medium.